WALUTA INTERNETOWA: TECHNOLOGIA BITCOINA

Marian Srebrny
Instytut Podstaw Informatyki
Polska Akademia Nauk
Warszawa
marians@ipipan.waw.pl

3 października 2016

PLAN PREZENTACJI

Nic w tej prezentacji nie stanowi porady inwestycyjnej, prawnej ani podatkowej.

Krótka prezentacja krajobrazu najważniejszych i najciekawszych zagadnień i zdarzeń dot. protokołu Bitcoin, jego projektu i możliwości złamania.

- **HISTORIA BITCOINA – e-ZŁOTO**
- **GŁÓWNY BOHATER: KRYPTOGRAFICZNE FUNKJE SKRÓTU (ang. HASH FUNCTIONS)**
- **POJĘCIE DOWODU WYKONANIA PRACY (ang. PROOF-OF-WORK)**
- **BEZ PODMIOTU OBDARZONEGO ZAUFANIEM - WSPÓLNE WIELOSTRONNE ZARZĄDZANIE PRZEZ CONSENSUS WIĘKSZOŚCI**
- **PUBLICZNY REJESTR WSZYSTKICH TRANSAKCJI**
- **WYBRANE SZCZEGÓŁY TECHNOLOGII:**
  WYDOBYWANIE BITCOINÓW,
  ZACHĘTY (ang. INCENTIVES),
  ADRESY/KONTA, TRANSAKCJE, e-PODPISY, itd.

SZCZYPTA HISTORII BITCOINA

GŁÓWNI PROGRAMIŚCI
(ang. CORE DEVELOPERS):

- **Satoshi Nakamoto – klucz publiczny PGP**
- **Gavin Andresen - gavinandresen@gmail.com - PGP**
- **Pieter Wuille - pieter.wuille@gmail.com - PGP**
- **Nils Schneider - nils.schneider@gmail.com - PGP**
- **Jeff Garzik - jgarzik@bitpay.com - PGP**
- **Wladimir J. van der Laan - laanwj@gmail.com - PGP**
- **Gregory Maxwell - greg@xiph.org - PGP**

(Patrz *Bitcoin development*, http://bitcoin.org/en/development.)

„RESPONSIBILITY DISCLOSURE
If you find a vulnerability related to Bitcoin (…), critical vulnerabilities that are too sensitive for unencrypted email should be sent to one or more of the core developers, encrypted.

VIDEO http://bitcoin.org/en/

CZYM JEST BITCOIN?

Można wprowadzić to jako:

- **Waluta cyfrowa/internetowa (alternatywna wobec rządowych i bankowych)**
- **Towar wymienny**
- **Internetowa gorączka złota**

- **Technologia naprawdę demokratycznej globalnej ekonomii/społeczeństwa**
- **Cyfrowy system finansowy**
- **System szybkich płatności, przekazów i transakcji**
- **Innowacyjna sieć płatności**
- **Technologiczna platforma o wielu możliwościach nieobecnych dotąd**
- **Komputerowy program współbieżny (sieciowy)**
- **Wielopodmiotowy protokół kryptograficzny**

W TEJ PREZENTACJI

Bitcoin to PROTOKÓŁ KRYPTOGRAFICZNY, motywowany ideą cyfrowego złota.

Wydobywa się nowe bitcoiny podobnie do złota – ogromnym nakładem pracy komputerów, mocy obliczeniowej i prądu elektrycznego.

Pierwszy system e-pieniędzy z szerokim kręgiem użytkowników. Ale bez instytucji wydawcy (emitenta).

Program komputerowy równoprawnych podmiotów, z otwartym źródłem.

Wiarygodność zabezpieczeń kryptograficznych oparta na założeniu: większość uczestników jest uczciwa.

Bitcoin z dużej litery oznacza system, oprogramowanie i sieć komputerów, a bitcoin z małej litery to jednostka waluty.

WYDOBYWANIE BITCOINÓW

Wydobywcy (kopacze, górnicy, ang. miners)

próbują znaleźć rozwiązanie następującej nierówności:

$$a \bullet x < c$$

$$f(a,x) < c$$

właściwie $\text{sha256}(\text{sha256}(a,x)) < c$

gdzie

x **jest niewiadomą (której wartość trzeba znaleźć),**

a **jest liczbą kodującą całą dotychczasową historię wszystkich transakcji w bitcoinach,**

c **jest pewną liczbą specjalnie dobraną i uaktualnianą co 2 tyg.,**

f **natomiast jest funkcją nieodwracalną.**

WYDOBYWANIE BITCOINÓW

Wydobywcy (kopacze, górnicy, ang. miners)

próbują znaleźć rozwiązanie następującej nierówności:

$$\text{sha256}(\text{sha256}(a,x)) < c$$

gdzie

***x* jest niewiadomą (której wartość trzeba znaleźć),**

***a* jest liczbą kodującą całą dotychczasową historię wszystkich transakcji w bitcoinach,**

***c* jest pewną liczbą specjalnie dobraną i uaktualnianą co 2 tyg.,**

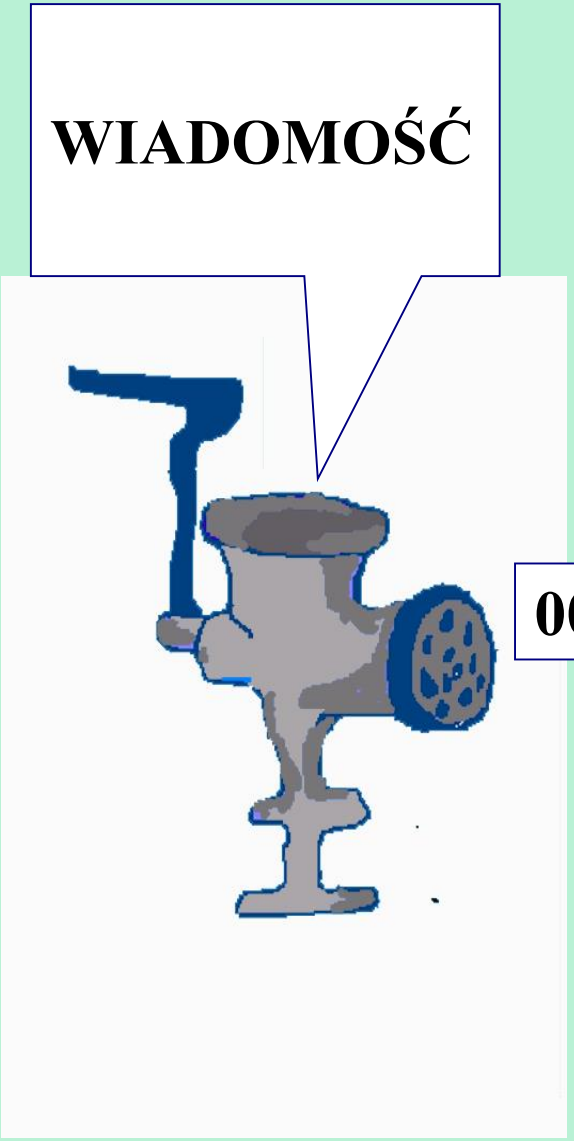
***f* natomiast jest funkcją nieodwracalną.**

To jest loteria!

Wynik funkcji skrótu jest nieprzewidywalny,

więc górnicy muszą próbować losowo bardzo wiele razy, by trafić na rozwiązanie (dla *x*). Nikt dziś nie zna żadnej innej metody rozwiązywania tej nierówności.

KRYPTOGRAFICZNA FUNKCJA SKRÓTU SHA-256



JEDNOZNACZNE
I NIEODWRACALNE

NAGRODA

Nagroda za znalezienie rozwiązania - 12,5 bitcoinów (na dziś).
Tylko jedna osoba co 10 minut średnio zarabia w ten sposób.
Ten kto pierwszy znajdzie rozwiązanie owej nierówności.
Górnicy konkurują o to.
Ich komputery zgadują i sprawdzają miliardy liczb-kandydatów.
To wymaga mnóstwo czasu, sprzętu i prądu.
Większy komputer - większa moc obliczeniowa - jest lepszy.

Prawdziwy górnik wydobywa złoto, które nie należało do nikogo.
Podobnie w wydobywaniu bitcoinów, protokół nagradza pracę górnika nowo generowanymi bitcoinami, które nie należały do nikogo.

Znalezione rozwiązanie i nagroda są wpisywane do rejestru jako następny blok wraz ze wszystkimi nowymi transakcjami, jeśli są poprawne. Sprawdzają to też następni górnicy.
To mechanizm (technika) consensusu!

PUBLICZNY REJESTR

Tradycyjne waluty działają na zasadzie zaufania do banków, wydawców kart kredytowych czy usługodawców (np. PayPal) — które przetwarzają transakcje i uaktualniają stany kont. To zapobiega wydawaniu tych samych pieniędzy dwa lub więcej razy. Ogólna idea: nadzór, centralna władza, Wielki Brat. Bitcoin nie ma centrali!

Zamiast tego w Bitcoinie jest publiczny rejestr (ang. ledger) wszystkich transakcji, nazywany łańcuchem bloków (ang. block chain). Każda transakcja, która kiedykolwiek miała miejsce jest zapisana i przechowywana w publicznie dostępnym, rozproszonym na wszystkie komputery w sieci Bitcoina ogromnym rejestrze (ang. Distributed Ledger).

Każdy może ściągnąć sobie kopię tego rejestru, ale by dopisać cokolwiek trzeba być górnikiem. Tzn. rozwiązać nierówność i potwierdzić poprawność nowych transakcji, które wtedy zostaną dopisane do rejestru.

ADRESY/KONTA I TRANSAKCJE

Adres Bitcoina to w zasadzie klucz publiczny użytkownika.
Wygląda tak:
16UwLL9Risc3QfPqBUvKofHmBQ7wMtjvM
Por.
https://en.bitcoin.it/wiki/Technical_background_of_Bitcoin_addresses

Transakcja to podpisane cyfrowo przekazanie własności bitcoinów do nowego adresata wysłane do sieci i dopisane do rejestru. Zawiera dane o poprzednich transakcjach tymi bitcoinami i adresy nadawcy i beneficjenta (adresata).

Prywatność użytkownika to właściwie jedynie pseudonim (klucz publiczny).

W SUMIE:

kryptograficzne zabezpieczenia

na najwyższym poziomie możliwym obecnie.

PRZYSZŁOŚĆ TECHNOLOGII PUBLICZNEGO ROZPROSZONEGO REJESTRU ŁAŃCUCHA BLOKÓW (ang. DISTRIBUTED LEDGER TECHNOLOGY)

Na przykład

- **Księgi wieczyste, rejestr pojazdów, itp.**
- **Rozproszony system głosowania elektronicznego**

Zagadnienia do zbadania

- **Bezpieczeństwo polskich systemów Blik i Billon?**

  Możliwe transakcje przez GSM lub Bluetooth, nawet bez Internetu.

ŹRÓDŁA

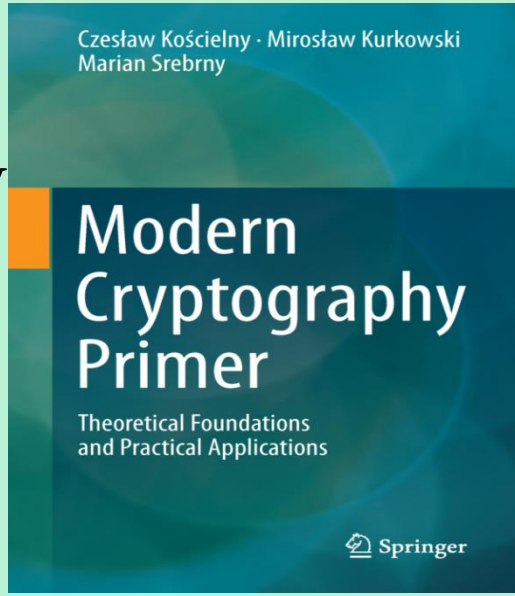
1. Satoshi Nakamoto *Bitcoin*, Jan 9, 2009, http://bitcoin.org/bitcoin.pdf [Dostęp: 2 stycznia 2016]
2. *Bitcoin*, http://bitcoin.org/en/ [Dostęp: 2 stycznia 2016]
3. *Protocol specification*, https://en.bitcoin.it/wiki/Protocol_specification [Dostęp: 4 czerwca 2014]
4. *Bitcoin_development*, http://bitcoin.org/en/development [Dostęp: 2 stycznia 2016]
4. SHA-256 jest opisana szczegółowo w: Secure Hash Standard, NIST FIPS PUB 180-3, U.S. Dept of Commerce, October 2008.

ŹRÓDŁA Z KRYPTOGRAFII

Ross Anderson *Security Engineering*, *2008*
Dostępne za darmo z http://www.cl.cam.ac.uk/~rja14/book.html

Alfred Menezes, Paul van Oorschot, Scott Vanstone
Handbook of Applied Cryptography, CRC Press,
Dostępne za darmo z www.cacr.uwaterloo.ca/hac/

Cz.Kościelny, M.Kurkowski, M.Srebrny
Modern Cryptography Primer,
Springer-Verlag, 2013



DZIĘKUJĘ ZA UWAGĘ!

PYTANIA, UWAGI, KOMENTARZE ?